(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 16 015 A 1**

(51) Int. Cl.[6]: G 06 K 19/073

(21) Aktenzeichen: 197 16 015.8
(22) Anmeldetag: 17. 4. 97
(43) Offenlegungstag: 29. 10. 98

DE 197 16 015 A 1

(71) Anmelder:
International Business Machines Corporation, Armonk, N.Y., US

(74) Vertreter:
Rach, W., Dr., Pat.-Ass., 70569 Stuttgart

(72) Erfinder:
Schaal, Albert, 72076 Tübingen, DE; Hänel, Walter, Dipl.-Phys., 71088 Holzgerlingen, DE; Deindl, Michael, Dipl.-Inf., 71034 Böblingen, DE

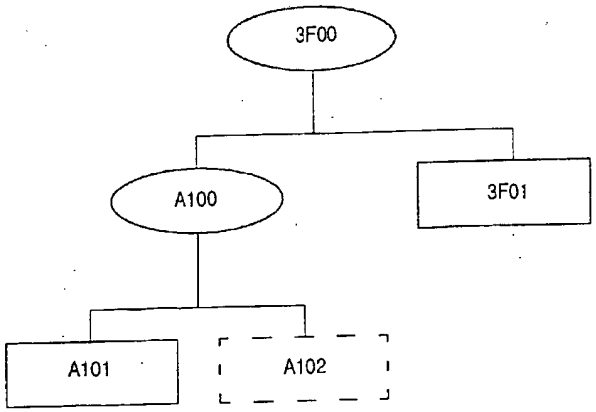
(56) Entgegenhaltungen:
DE 1 95 36 206 A1
DE 1 95 35 770 A1
DE 44 36 697 A1
DE 38 05 291 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Einbringen von Information auf einer Chipkarte

(57) Die Erfindung bezieht sich auf ein Verfahren zum Einbringen von Information, insbesondere von Anwendungsinformation, auf einer Chipkarte, die einen Speicher mit einem Verzeichnis aufweist, wobei bei dem Verfahren die Information auf die Chipkarte übertragen wird, der Inhalt des Speichers gemäß der Information verändert wird, ein elektronischer Fingerabdruck einer Gesamtinformation, welche die Information und eine Zusatzinformation über die Veränderung des Inhalts umfaßt, berechnet wird, der elektronische Fingerabdruck mit wenigstens einem weiteren elektronischen Fingerabdruck verglichen wird, und die Veränderung des Inhalts des Speichers der Chipkarte aktiviert wird, wenn beim Vergleichen eine Übereinstimmung zwischen dem elektronischen Fingerabdruck und dem wenigstens einen weiteren elektronischen Fingerabdruck festgestellt wird.



DE 197 16 015 A 1

Beschreibung

Die Erfindung betrifft das Einbringen von Information, insbesondere von Anwendungsinformation, auf einer Chipkarte, die einen Speicher mit einem Verzeichnis aufweist.

Seit Mitte der 80er Jahre finden Chipkarten in immer mehr Bereichen des täglichen Lebens Anwendung. Dieser Erfolg der Chipkarten beruht im wesentlichen auf ihrer hohen Manipulationssicherheit und ihrer Zuverlässigkeit. Desweiteren ist mittels der Programmierbarkeit der Chips auf der Chipkarte eine große Flexibilität für eine Vielzahl von Anwendungen der Chipkarte gewährleistet.

Die Herstellung einer Chipkarte bis zum Zeitpunkt, zu dem sie an einen Benutzer ausgegeben werden kann, ist in Rankl/Effing: Handbuch der Chipkarten, Karl Hanser Verlag, 1996, beschrieben. Nachdem ein Modul mit dem Halbleiterchip in die Chipkarte eingebettet wurde, werden anschließend globale Daten und persönliche Daten des zukünftigen Kartenbenutzers auf der Chipkarte eingebracht. Hierbei werden vom Herausgeber der Chipkarte immer häufiger mehrere Anwendungen gleichzeitig auf der Chipkarte eingebracht.

Die innere Struktur der Chipkarte folgt im wesentlichen der Norm ISO 7816/4. Üblicherweise sind die Daten und/oder der Code, welcher zu einer Anwendung gehört, in Dateien untergebracht. Die Dateien befinden sich in einem Verzeichnis im Speicher der Chipkarte. Die Dateien und das Verzeichnis werden von dem Kartenherausgeber auf der Chipkarte eingebracht. Soll nun von einem Anwendungsanbieter eine neue Anwendung auf eine bereits herausgegebene Chipkarte aufgebracht werden, so ist dem Sicherungssystem der Chipkarte besondere Aufmerksamkeit zu widmen. Dies gilt insbesondere, wenn es sich um Anwendungen handelt, welche sich nicht unter der Kontrolle des Kartenherausgebers befinden. Bringt ein Anwendungsanbieter Daten und/oder Code selbständig auf der Chipkarte auf, so besteht die Gefahr, daß die aufgebrachten Daten und/oder der aufgebrachte Code die Sicherheit der Chipkarte untergraben. Dies kann beabsichtigt sein, wenn man dem Anwendungsanbieter ein Interesse unterstellt, Anwendungen des Kartenherausgebers oder anderer Anwendungsanbieter auszuspionieren. Aber auch eine ungewollte Beeinträchtigung des Sicherungssystems der Chipkarte kann hervorgerufen werden, insbesondere durch das fehlerhafte Aufbringen neuer Anwendungen.

Aus DE 38 07 997 ist ein Verfahren zum Aufbringen von Daten auf eine Chipkarte bekannt. Die Chipkarte weist einen Speicher auf, welcher in mehrere Teilbereiche unterteilt ist. Einer dieser Teilbereiche ist als ein geschützter Teilbereich ausgebildet. In dem geschützten Teilbereich werden Adressinformationen und Fehlerprüfcodes für andere Teilbereiche gespeichert. Der geschützte Teilbereich wird geschützt, indem der Mikroprozessor der Chipkarte so programmiert ist, daß er einen Zugriff eines Terminals zu dem geschützten Teilbereich verhindert. Hierdurch können Informationen, die in dem geschützten Teilbereich angeordnet sind, gegen den Zugriff eines nicht berechtigten Anwendungsanbieters geschützt werden.

Die deutsche Patentanmeldung mit dem Aktenzeichen 196 26 339 offenbart ein Verfahren zum sicheren Laden von Anwendungen und Daten auf Chipkarten. Bei diesem Verfahren wird eine Kennung vergeben. Die Kennung wird vor einer Ausführung eines Kommandos, mittels dem die Daten in einen Teilbereich der Chipkarte eingebracht werden sollen, ermittelt. Bei der Ermittlung der Kennung wird festgestellt, ob eine Ausführung des Kommandos in dem Teilbereich zugelassen ist. Die Ausführung des Kommandos wird verhindert, wenn bei der Ermittlung der Kennung festgestellt wird, daß die Ausführung des Kommandos in dem Teilbereich nicht zugelassen ist.

Hierdurch kann die Ausführung bestimmter Kommandos, insbesondere von Kommandos zum Einbringen von Anwendungen auf der Chipkarte, auf bestimmte Teilbereiche begrenzt werden.

Bei einem weiteren bekannten Verfahren zum Einbringen von Anwendungsinformation auf einer Chipkarte wird die Information mit einer elektronischen Unterschrift versehen. Die elektronische Unterschrift wird hierbei mittels einem kryptographischen Schlüssel aus einem elektronischen Fingerabdruck der Information berechnet. Die Information und die elektronische Unterschrift werden auf die Chipkarte übertragen. Auf der Chipkarte wird mit Hilfe eines weiteren kryptographischen Schlüssels nochmals eine elektronische Unterschrift der Information, welcher auf die Chipkarte übertragen wurde, berechnet. Hierdurch kann anschließend überprüft werden, ob die auf die Chipkarte übertragene elektronische Unterschrift und die auf der Chipkarte berechnete elektronische Unterschrift übereinstimmen. Ist das der Fall, so wurde die Information fehlerfrei auf die Chipkarte übertragen. Manipulationen werden bei diesem bekannten Verfahren dadurch verhindert, daß der weitere kryptografische Schlüssel durch eine vertrauenswürdige Instanz zertifiziert wird.

Mit Hilfe des bekannten Verfahrens, welches im letzten Abschnitt beschrieben wurde, ist es nicht möglich zu überprüfen, ob die Information an dem ihr zugewiesenen Ort im Speicher der Chipkarte angeordnet wurde. Umfaßt eine Anwendung, die auf die Chipkarte aufgebracht werden soll, Daten und Code, so kann es notwendig sein, diese Daten und den Code auf verschiedene Dateien im Verzeichnis zu verteilen. Mit dem bekannten Verfahren kann dann überprüft werden, ob die Daten und der Code ohne Manipulation derselben, auf die Chipkarte übertragen wurden. Es ist jedoch nicht möglich, mit dem bekannten Verfahren festzustellen, ob die Daten und der Code ordnungsgemäß in den verschiedenen Dateien angeordnet wurden.

Es ist deshalb die Aufgabe der vorliegenden Erfindung, eine verbesserte Möglichkeit zum Einbringen von Information in einer Chipkarte zu schaffen.

Diese Aufgabe wird gemäß den unabhängigen Ansprüchen 1 und 10 gelöst.

Der wesentliche Vorteil, welcher mit der Erfindung gegenüber dem Stand der Technik erreicht wird, besteht darin, daß zusätzlich zur Überprüfung der fehlerfreien Übertragung der Information auf die Chipkarte auch überprüft wird, daß die Information gemäß einer Zusatzinformation in die Chipkarte integriert wird. Nur, wenn beim Verändern des Inhalts des Speichers die Zusatzinformation ordnungsgemäß beachtet wurde, kann die eingebrachte Information zur Ausführung einer Anwendung genutzt werden.

Das Einbringen von Information in einem für diese nicht zugelassenen Bereich des Speichers der Chipkarte wird so verhindert. Dies erhöht den Sicherheitsstandard der Chipkarte.

Bei einer zweckmäßigen Ausführung der Erfindung wird der wenigstens eine weitere elektronische Fingerabdruck auf der Chipkarte gespeichert. Hierdurch kann der elektronische Fingerabdruck, welcher zur Überprüfung der auf die Chipkarte übertragenen Information benutzt wird, zu einem beliebigen Zeitpunkt auf der Chipkarte angeordnet werden, um dann später beim Einbringen der Information benutzt zu werden. Es können zu einem Zeitpunkt mehrere elektronische Fingerabdrücke auf der Chipkarte angeordnet werden, wobei die zu den Fingerabdrücken jeweils gehörenden Informationen zu verschiedenen Zeitpunkten auf der Chipkarte eingebracht werden können.

Vorteilhaft kann vorgesehen sein, daß der wenigstens eine weitere elektronische Fingerabdruck mittels einem kryptographischen Schlüssel aus einer elektronischen Unterschrift ermittelt wird. Dies erlaubt die Einbeziehung einer weiteren Sicherheitsmaßnahme, das Ver- und Entschlüssein, beim Einbringen der Information, wodurch der Sicherheitsstandard weiter verbessert wird.

Bei einer zweckmäßigen Weiterbildung der Erfindung werden beim Verändern des Inhaltes des Speichers Daten und/oder ein Code in einer Datei im Verzeichnis des Speichers angeordnet, wobei die Zusatzinformation eine Pfadangabe für die Datei umfaßt. Hierdurch wird mittels der Zusatzinformation die Anordnung von Daten und/oder von Code in einer bestimmten Datei des Speichers gewährleistet.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß vor dem Anordnen der Daten und/oder des Codes in der Datei dieselbe erzeugt wird, wodurch die für das Einbringen der Information notwendige Datei unmittelbar im Zusammenhang mit dem Einbringen erzeugt wird, und ein Schritt zum vorherigen Erstellen von Dateien zum Einbringen von Information eingespart wird.

Vorteilhaft kann vorgesehen sein, daß vor dem Anordnen der Daten und/oder des Codes in der Datei das Verzeichnis erzeugt wird, wodurch beim Einbringen der Information eine Erzeugung zusätzlicher Verzeichnisse im Speicher der Chipkarte ermöglicht wird.

Zweckmäßig kann die Zusatzinformation eine Information über eine Spezifikation der Datei, insbesondere über eine Identifikation und eine Größe der Datei, umfassen. Hierdurch wird gewährleistet, daß die Daten und/oder der Code nur in Dateien angeordnet werden können, die Merkmale aufweisen, wie sie für die Benutzung der Daten und/oder des Codes im Rahmen einer Anwendung der Chipkarte notwendig sind.

Bei einer vorteilhaften Weiterbildung der Erfindung umfaßt die Zusatzinformation eine Information über das Verzeichnis, wodurch überprüft wird, ob das Verzeichnis die für die Nutzung der Daten und/oder des Codes notwendigen Eigenschaften aufweist. Zu diesen Eigenschaften gehört insbesondere eine entsprechende Dateistruktur des Verzeichnisses.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß die Zusatzinformation eine Information über weitere Dateien in dem Verzeichnis umfaßt. Hierdurch wird überprüft, ob weitere Dateien in dem Verzeichnis, in welchem die Daten und/oder der Codes eingebracht werden, die für die Nutzung der Daten und/oder des Codes erforderlichen Merkmale aufweisen.

Für die zweckmäßigen Ausführungen der Erfindung als Chipkarte in den Ansprüchen 10 bis 16 gelten die im Zusammenhang mit den dazugehörigen Verfahrensansprüchen genannten Vorteile entsprechend.

Die Erfindung wird im folgenden anhand einer Zeichnung näher beschrieben. Hierbei zeigt:

Fig. 1 eine schematische Darstellung eines Verzeichnisses im Speicher einer Chipkarte.

Gemäß **Fig.** 1 weist das Verzeichnis im Speicher der Chipkarte ein Hauptverzeichnis 3F00 auf. In diesem Hauptverzeichnis ist eine Registrierungsdatei 3F01 angeordnet. Das Hauptverzeichnis weist weiterhin ein Anwendungsverzeichnis A100 auf. In dem Anwendungsverzeichnis A100 befindet sich die Binärdatei A101, welche Daten umfaßt.

Das Verzeichnis mit dem Hauptverzeichnis 3F00, der Registrierungsdatei 3F01, dem Anwendungsverzeichnis A100 und der Binärdatei A101 wurde vom Herausgeber der Chipkarte auf derselben eingebracht. Diese vom Herausgeber der Chipkarte erstellte Struktur des Verzeichnisses im Speicher der Chipkarte ist so konfiguriert, daß eine Anwendung A100 eines Anwendungsanbieters 1 ausführbar ist.

Die Anwendung A100 soll nun um ein neues Kommando erweitert werden. Hierzu hat der Anwendungsanbieter 1 einen Kommandocode erzeugt. Dieser Kommandocode muß der Anwendungsanbieter 1 vom Kartenherausgeber zertifizieren lassen. Dies bedeutet, daß der Kartenherausgeber bestätigt, daß der Kommandocode, sowie er vom Anwendungsanbieter 1 erstellt wurde, an einen bestimmten Ort in dem Verzeichnis der Chipkarte eingebracht werden kann.

Der vom Anwendungsanbieter erzeugte Kommandocode soll in einer Binärdatei A102 angeordnet werden. Gemäß **Fig.** 1 befindet sich die Binärdatei A102 im Anwendungsverzeichnis A100. Beim Einbringen des Kommandocodes durch den Anwendungsanbieter 1 muß sichergestellt werden, daß der Kommandocode ordnungsgemäß in der Binärdatei A102 angeordnet wird. Es geht hierbei sowohl um die Vermeidung von ungewollten Fehlern beim Einbringen des Kommandocodes als auch um die Verhinderung bewußter Manipulationen, wenn man dem Anwendungsanbieter 1 ein Interesse an der Untergrabung des Sicherheitsstandards der Chipkarte unterstellt.

Um ein ordnungsgemäßes Einbringen des Kommandocodes in die Binärdatei A102 zu gewährleisten, wird im Rahmen der Zertifizierung durch den Kartenherausgeber eine Information gebildet, die einerseits den Kommandocode umfaßt und andererseits eine Zusatzinformation aufweist, welche eine Pfadangabe für die Binärdatei A102 in dem Verzeichnis der Chipkarte umfaßt. Anschließend wird ein elektronischer Fingerabdruck, insbesondere ein Hashwert, der Information berechnet. Dieser elektronische Fingerabdruck der Information wird durch den Kartenherausgeber in der Registrierungsdatei 3F01 abgelegt.

Zu einem beliebigen späteren Zeitpunkt kann nun der Karteninhaber das neue Kommando in die Anwendung A101 integrieren. Hierbei kann es notwendig sein, die Binärdatei A102 beim Einbringen des Kommandocodes neu zu erzeugen. Aber auch ein Überschreiben von altem Code in der Binärdatei A102 mit dem neuen Kommandocode ist ausführbar. Es ist außerdem denkbar, daß beim Einbringen eines neuen Codes ein neues Verzeichnis mit wenigstens einer Datei erzeugt werden muß.

Zum Einbringen des neuen Kommandocodes wird die Chipkarte in ein Terminal des Anwendungsanbieters 1 eingeführt. Anschließend wählt der Karteninhaber eine Funktion des Terminals mittels welcher der Kommandocode auf die Chipkarte übertragen wird. Nachdem der Kommandocode in die Binärdatei A102 geschrieben wurde, wird die Binärdatei A102 als nicht aktiv gekennzeichnet. Dies geschieht, indem der Status der Binärdatei entsprechend angepaßt wird. Der Status einer Datei kann beispielsweise in einem Byte innerhalb eines File-Headers gespeichert werden.

Um den Kommandocode im Rahmen der Anwendung A101 nutzen zu können, muß nun überprüft werden, ob der Kommandocode ordnungsgemäß in die Chipkarte integriert wurde. Ist dies der Fall, so wird der Status der Binärdatei A102 anschließend so verändert, daß er anzeigt, daß die Datei A102 aktiv ist.

Um das ordnungsgemäße Einbringen des Kommandocodes zu überprüfen, wird auf der Chipkarte ein elektronischer Fingerabdruck einer Information gebildet, die den auf die Chipkarte übertragenen Kommandocode und eine Pfadangabe für die Binärdatei A102 umfaßt. Die Information wird gebildet, indem die Pfadangabe an den Kommandocode angehängt wird. Die Pfadangabe kann beispielsweise dadurch gebildet werden, daß die drei Angaben 3F00/A100/A102 aneinandergereiht werden. Alternativ kann die Pfadangabe auch mit einem laut ISO 7816-5 definierten Namen begin-

nen. Dies ist möglich, da der Name einer Anwendung laut ISO 7816-5 eindeutig sein muß. Wurde der Kommandocode ordnungsgemäß auf der Chipkarte eingebracht, so ist die auf der Chipkarte gebildete Information identisch zu der Information, die vom Kartenherausgeber bei der Zertifizierung des Kommandocodes des Anwendungsanbieters 1 erzeugt wurde.

Der auf der Chipkarte berechnete elektronische Fingerabdruck wird nun mit dem Fingerabdruck verglichen, welchen der Kartenherausgeber in der Registrierungsdatei 3F01 abgelegt hat. Sind in der Registrierungsdatei 3F01 mehrere elektronische Fingerabdrücke verschiedener Anwendungsanbieter abgelegt, so wird der auf der Karte berechnete elektronische Fingerabdruck nacheinander mit den weiteren elektronischen Fingerabdrücken in der Registrierungsdatei 3F01 verglichen, bis festgestellt wird, ob der auf der Karte berechnete elektronische Fingerabdruck mit einem der weiteren Fingerabdrücke übereinstimmt, oder bis festgestellt wird, daß keine Übereinstimmung gefunden wurde. Wird eine Übereinstimmung mit einem der weiteren elektronischen Fingerabdrücke festgestellt, so wird der Kommandocode in der Binärdatei A102 aktiviert, d. h. er ist im Rahmen der Anwendung A100 nutzbar. Wird keine Übereinstimmung festgestellt, so wird die Binärdatei A102 nicht aktiviert und eine Fehlermeldung wird erzeugt.

Neben der Pfadangabe der Binärdatei A102 können bei der Berechnung des elektronischen Fingerabdruckes der Information bei der Zertifizierung durch den Kartenherausgeber und bei der Berechnung des elektronischen Fingerabdruckes auf der Chipkarte jeweils auch weitere Eigenschaften der Binärdatei A102, des Anwendungsverzeichnisses A100 und/oder des Verzeichnisses im Speicher der Chipkarte einbezogen werden. So können beispielsweise Informationen über die Größe und die Art der Binärdatei A102 bei der Berechnung des elektronischen Fingerabdruckes einbezogen werden.

Um sicherzustellen, daß der Kommandocode, welcher in die Binärdatei A102 eingebracht wird, in einer vollständigen Dateistruktur des Anwendungsverzeichnisses A100 eingebracht wurde, können bei der Berechnung des elektronischen Fingerabdruckes noch folgende Parameter für jede Datei im Anwendungsverzeichnis A100 aufgenommen werden:

- Dateiidentifikation,
- Größe der Datei,
- Zugriffsrechte auf die Datei gemäß CEN 726.

Desweiteren können bei der Erstellung der Information, für welche anschließend ein elektronischer Fingerabdruck berechnet wird, Merkmale und Eigenschaften des Anwendungsverzeichnisses A100 selbst integriert werden.

Es ist stets darauf zu achten, daß die Parameter der Dateien und/oder des Anwendungsverzeichnisses bei der Erstellung der Information durch den Kartenherausgeber zur Zertifizierung und bei der Erstellung der Information auf der Chipkarte jeweils in derselben Reihenfolge angeordnet werden. Nur so kann sichergestellt werden, daß die jeweiligen elektronischen Fingerabdrücke miteinander vergleichbar sind.

Verfügt die Chipkarte, auf welche der neue Kommandocode übertragen werden soll, über einen Prozessor, der asymmetrische Kryptographie unterstützt, so kann bei der Überprüfung des ordnungsgemäßen Einbringens des Kommandocodes die Berechnung einer elektronischen Unterschrift genutzt werden. Bei dieser Weiterbildung des Verfahrens überträgt der Kartenherausgeber im Rahmen der Zertifizierung an Stelle des elektronischen Fingerabdrucks eine elektronische Unterschrift in die Registrierungsdatei 3F01, wobei diese elektronische Unterschrift mit Hilfe eines geheimen Schlüssels aus dem elektronischen Fingerabdruck der Information gebildet wurde. Die Information umfaßt auch bei dieser Ausführung den Kommandocode und eine Pfadangabe für und/oder andere Angaben über die Binärdatei A102.

Bei der Überprüfung des ordnungsgemäßen Einbringens des Kommandocodes in die Binärdatei A102 auf der Chipkarte wird ein öffentlicher Schlüssel benutzt, um die vom Kartenherausgeber in die Registrierungsdatei 3F01 übertragene elektronische Unterschrift zu entschlüsseln. Ergebnis der Entschlüsselung mittels dem öffentlichen Schlüssel ist ein elektronischer Fingerabdruck. Dieser elektronische Fingerabdruck wird dann mit dem auf der Chipkarte ermittelten elektronischen Fingerabdruck verglichen. Je nachdem, ob eine Übereinstimmung festgestellt wird oder nicht, wird der auf die Chipkarte übertragene Kommandocode anschließend aktiviert oder nicht.

Auch bei der Verwendung der asymmetrischen Kryptographie können bei der Erstellung der Information, aus welcher anschließend der elektronische Fingerabdruck und die elektronische Unterschrift berechnet werden, Parameter der Dateien des Anwendungsverzeichnisses oder des Anwendungsverzeichnisses selbst einbezogen werden.

Ein Befehl, mittels dem die Überprüfung des ordnungsgemäßen Einbringens des Kommandocodes in die Binärdatei A102 und die Aktivierung des Kommandocodes bei Feststellung eines ordnungsgemäßen Einbringens ausgeführt wird, ist gemäß ISO 7816-4 strukturierbar und weist insbesondere folgende Parameter auf:

- Kodierung des Befehls,
- Dateiidentifikation für die Datei, auf welche der Befehl angewendet wird,
- Schlüsselidentifikation für den zu benutzenden kryptografischen Schlüssel, wenn asymmetrische Kryptografie genutzt wird, und
- Länge der folgenden Daten und/oder des folgenden Codes.

Diese Parameter sind in einem Befehl-Header angeordnet. Mittels einem Befehls der die beschriebenen Parameter umfaßt wird der auf die Chipkarte übertragene Code verifiziert und anschließend aktiviert.

Neben der beschriebenen Ergänzung oder Erweiterung eines Anwendungsverzeichnisses A100 ist es mit Hilfe des beschriebenen Verfahrens auch möglich, neue Anwendungsverzeichnisses in ihrer Gesamtheit zu erzeugen und deren ordnungsgemäßes Einbringen im Speicher der Chipkarte zu überprüfen. Zur Erzeugung von Anwendungsverzeichnissen und den darin enthaltenen Dateien werden Standardkommandos, beispielsweise gemäß CEN 726, genutzt.

Während des Verlaufs des Einbringens eines neuen Anwendungsverzeichnisses wird diese neue Anwendungsverzeichnis als temporäres Anwendungsverzeichnis, welches noch nicht benutzt werden darf, gekennzeichnet.

Sollte beim Aufbau eines entsprechenden Anwendungsverzeichnisses und seiner Dateien eine Unterbrechung auftreten, insbesondere durch Stromausfall oder Herausnehmen der Chipkarte aus dem Terminal, so wird beim nächsten Einführen der Chipkarte in ein Terminal und dem hierbei ausgeführten Reset automatisch das dem zu erzeugenden Anwendungsverzeichnis übergeordnete Verzeichnis ausgewählt. In **Fig.** 1 ist das Verzeichnis 3F00 das dem Anwendungsverzeichnis A100 übergeordnete Verzeichnis. Mit Hilfe des automatischen Auswählens des übergeordneten Verzeichnisses wird verhindert, daß auf das nicht vollständig erzeugte

Anwendungsverzeichnis, welches noch als temporäres Anwendungsverzeichnis gekennzeichnet ist, zugegriffen wird. Mit Hilfe der "temporär"-Kennzeichnung können unvollständig erzeugte Anwendungsverzeichnisse im Rahmen des Reset der Chipkarte beim erneuten Einbringen in ein Terminal gelöscht werden, wenn eine Suche nach "temporär" gekennzeichneten Anwendungsverzeichnissen durchgeführt wird.

Das Einbringen des neuen Anwendungsverzeichnisses kann beispielsweise mit einem Befehl ausgeführt werden, der im wesentlichen dem CREATE-Befehl aus dem Standard CEN 728 entspricht. Der CREATE-Befehl wird um folgende Eigenschaften erweitert:

- Es können nur Anwendungsverzeichnisse erzeugt werden, die einen Namen aufweisen.
- Das neue Anwendungsverzeichnis wird während seiner Erzeugung als "temporär" gekennzeichnet.
- Nach Abschluß der Erzeugung wird das neue Anwendungsverzeichnis automatisch selektiert.

Ist die Erzeugung eines Anwendungsverzeichnisses mit seinem Dateien, beispielsweise das Anwendungsverzeichnis A100 mit den Dateien A101 und A102, erfolgreich abgeschlossen worden, so kann anschließend mit Hilfe des beschriebenen Verfahrens, bei welchem ein elektronischer Fingerabdruck und/oder eine elektronische Unterschrift- berechnet werden, überprüft werden, ob das Anwendungsverzeichnis und seine Dateien ordnungsgemäß auf der Chipkarte eingebracht wurden. Hierzu werden beispielsweise Informationen über die Anzahl der im Anwendungsverzeichnis enthaltenen Dateien und deren strukturelle Verteilung bei der Berechnung des elektronischen Fingerabdruckes oder der elektronischen Unterschrift gemäß dem beschriebenen Verfahren einbezogen.

Ein Befehl zur Ausführung der Verifizierung des Einbringens des Anwendungsverzeichnisses kann wiederum vorteilhaft gemäß ISO 7816-4 strukturiert sein.

Patentansprüche

1. Verfahren zum Einbringen von Information, insbesondere von Anwendungsinformation, auf einer Chipkarte, die einen Speicher mit einem Verzeichnis aufweist, wobei das Verfahren die folgenden Verfahrensschritte umfaßt:
   a) Übertragen der Information auf die Chipkarte,
   b) Verändern eines Inhaltes des Speichers gemäß der Information,
   c) Berechnen eines elektronischen Fingerabdrucks einer Gesamtinformation, welche die Information und eine Zusatzinformation über die Veränderung des Inhaltes umfaßt,
   d) Vergleichen des elektronischen Fingerabdrucks mit wenigstens einem weiteren elektronischen Fingerabdruck, und
   e) Aktivieren der Veränderung des Inhaltes des Speichers der Chipkarte, wenn beim Vergleichen eine Übereinstimmung zwischen dem elektronischen Fingerabdruck und dem wenigstens einen weiteren elektronischen Fingerabdruck festgestellt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der wenigstens eine weitere elektronische Fingerabdruck auf der Chipkarte gespeichert wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der wenigstens eine weitere elektronische Fingerabdruck mittels einem kryptografischen Schlüssel aus einer elektronischen Unterschrift ermittelt wird.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß beim Verändern des Inhaltes des Speichers Daten und/oder ein Kode in einer Datei im Verzeichnis des Speichers angeordnet werden, wobei die Zusatzinformation eine Pfadangabe für die Datei umfaßt.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß vor dem Anordnen der Daten und/oder des Kodes in der Datei dieselbe erzeugt wird.
6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß vor dem Anordnen der Daten und/oder des Kodes in der Datei das Verzeichnis erzeugt wird.
7. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über eine Spezifikation der Datei, insbesondere über eine Identifikation und eine Größe der Datei, umfaßt.
8. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über das Verzeichnis umfaßt.
9. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über weitere Dateien in dem Verzeichnis umfaßt.
10. Chipkarte mit einem Speicher, wobei auf der Chipkarte ein elektronischer Fingerabdruck von wenigstens einer Gesamtinformation angeordnet ist, dadurch gekennzeichnet, daß die Gesamtinformation eine Information und eine Zusatzinformation umfaßt, wobei der Speicher mittels der Information, die unter Beflicksichtigung der Zusatzinformation auszuführen ist, veränderbar sind.
11. Chipkarte nach Anspruch 10, dadurch gekennzeichnet, daß der wenigstens eine elektronische Fingerabdruck in einem Verzeichnis im Speicher der Chipkarte gespeichert ist.
12. Chipkarte nach Anspruch 10, dadurch gekennzeichnet, daß der wenigstens eine elektronische Fingerabdruck mittels einem kryptografischen Schlüssels ermittelbar ist.
13. Chipkarte nach Anspruch 10, dadurch gekennzeichnet, daß bei der Veränderung des Speichers Daten und/oder ein Kode in einer Datei in einem Verzeichnis im Speicher der Chipkarte anordenbar sind, und daß die Zusatzinformation eine Pfadangabe für die Datei umfaßt.
14. Chipkarte nach Anspruch 13, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über eine Spezifikation der Datei, insbesondere über eine Identifikation und eine Größe der Datei, umfaßt.
15. Chipkarte nach Anspruch 13, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über das Verzeichnis umfaßt.
16. Chipkarte nach Anspruch 13, dadurch gekennzeichnet, daß die Zusatzinformation eine Information über weitere Dateien, die in dem Verzeichnis angeordnet sind, umfaßt.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 197 16 015 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 29. Oktober 1998

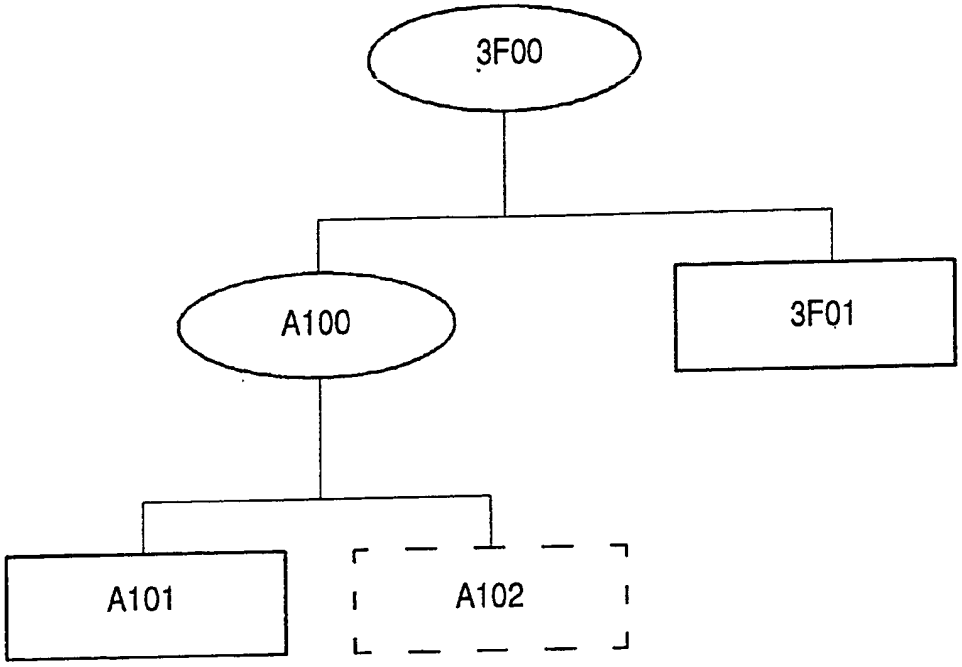


FIG. 1